Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2009)
"Energy and Technology for the Americas: Education, Innovation, Technology and Practice"
June 2-5, 2009, San Cristóbal, Venezuela.

Migración de Servicios de Servidores a Software Libre

Roberto Rodríguez Montoya
Universidad de las Ciencias Informáticas, Ciudad de La Habana, Cuba, robertom@uci.cu

Aned Corzo Leyva
Universidad de las Ciencias Informáticas, Ciudad de La Habana, Cuba, acorzo@uci.cu

Amaury Viera Hernández
Universidad de las Ciencias Informáticas, Ciudad de La Habana, Cuba, avhernandez@estudiantes.uci.cu

Leonardo de la Rosa
Universidad de las Ciencias Informáticas, Ciudad de La Habana, Cuba, ldelarosa@estudiantes.uci.cu

RESUMEN

En este trabajo se exponen las principales aplicaciones usadas en los servicios de servidores sobre software libre, alternativa que cada día, está cobrando auge y ganando aceptación en el mundo. Uno de los aspectos fundamentales del software libre es la naturaleza cooperativista de sus comunidades, que involucran a grandes redes de desarrolladores trabajando desde distintas localidades y compartiendo códigos para el mejoramiento del software, de forma de que se puede aprovechar esta ventaja y la gran reputación que tienen en el área de redes y seguridad. La migración de servicios de servidores hacia software libre, requiere de un estudio previo de del sistema a migrar, y de una planeación minuciosa de la misma, la sustitución de un sistema propietario a uno libre, debe hacerse de forma que todos los servicios continúen de igual forma, con el mínimos de cambios para el usuario final.

Palabras claves: DNS, GNU/Linux, LDAP, Migración, Software Libre

ABSTRACT

This document presents the main applications used in the servers services on free software, an alternative that every day is gaining acceptance in the world. One of the fundamental aspects of free software is the cooperative nature of their communities, involving large networks of developers working from different locations and sharing codes for the improvement of the software, so that we can take this advantage and the great reputation are in the area of networking and security. The servers services migration to free software, requires a prior study of the system to migrate, and a thorough planning of it, replacing a system owner one free, must be done so that all services continue the same way, the minimum changes to the end user.

Keywords: DNS, GNU / Linux, LDAP, Migration, Free Software

1. INTRODUCCIÓN

En nuestros días las soluciones tecnológicas basadas en software libre han crecido lo suficiente como para convertirse en una alternativa sólida que compite con carácter de igual con otras tecnologías de software propietario. Es probable que la batalla con preferencia de los clientes de servidores para empresas, esté en su mejor momento. Los servidores GNU/Linux pueden, a priori, asustar a algunos administradores; no obstante, este sistema operativo provee de paneles de control, para la gestión, configuración y administración de los servicios de servidores. De esta manera, sin conocimientos muy avanzados de este sistema, se puede gestionar, administrar y configurar un servidor de forma sencilla e intuitiva.

Los servidores GNU/Linux serán siempre más económicos que los servidores Microsoft Windows en aspectos como la actualización, desarrollo, soporte, mantenimiento del software y la prolongación de vida útil del hardware. La principal razón de ello es que existe una gran comunidad de software libre y aplicaciones gratuitas, o sea que se ahorra en lo referente al pago de las licencias. Tanto el sistema operativo GNU/Linux como las aplicaciones que normalmente corren sobre él, no requieren de licencias del proveedor. El objetivo que guía a este trabajo es el proceso de migración de servicios de servidores de forma automatizada en la medida de lo posible, permitiendo una mayor rapidez de trabajo, fiabilidad y menor probabilidad de error humano. Cada uno de las propuestas, estará sobre la base de mostrar una herramienta que permita migrar la configuración de los servicios telemáticos en cada servidor, siempre utilizando los servidores mas robustos y populares sobre software libre.

2. PROPUESTA DE MIGRACIÓN

La migración de los servidores propietarios hacia los servidores con sistema operativo GNU/Linux se hará gradualmente. Los servidores propietarios dejarán de funcionar una vez que el servidor con el sistema operativo GNU/Linux se encuentre instalado y correctamente migrado. Estas acciones serán completamente transparentes a los usuarios de la red, pues la misma funcionará con los mismos servicios de igual forma. La administración de estos servidores podría realizarse a través de los propios ficheros de configuración o a través de aplicaciones con interfaz gráfica que facilitan esta labor, como es el caso de *webmin*. Es necesario aclarar, que en el plan de migración debe contemplarse la planificación y estrategia de migración a utilizar.

MIGRACIÓN DE UN SERVIDOR DE DNS

Al hablar sobre la migración hacia un sistema de nombres de dominio o servidor de nombres y dominios como lo indican sus siglas en inglés “Domain Name Service”, se debe pensar en el BIND, el conocido Berkeley Internet Name Domain. Este el servidor de DNS más popular de Internet, es el más utilizado por su calidad y su característica de ser multiplataforma.

BIND no puede decirse que sea complicado sino que es un producto que funciona a través de una serie de archivos de configuración y que aún sin mucha práctica, está al alcance de cualquier tipo de usuario, además, existe grandes volúmenes de documentación sobre este producto, lo cual lo hace ser muy conocido y usado. El mismo cuenta con todas las características necesarias para ejecutar este tipo de software de servidor, la cuales son un espacio de nombres jerárquico para los hosts y las direcciones IP, un "resolvedor" o librería de rutinas que permite realizar consultas a esa base de datos, enrutamiento mejorado para el correo electrónico, un mecanismo para encontrar los servicios en una red, un protocolo para intercambiar información de nombres. El mismo brinda los servicios de resolución de nombres a direcciones IP y resolución inversa (de direcciones IP a nombres), así como listas de control de acceso, localización de servicios (registros SRV − RFC2052-), respuestas parametrizadas en función del origen de la petición conocidas como vistas, así como logs, que brindan diferentes informaciones acerca del funcionamiento del servidor y las peticiones al mismo.

Este servidor de nombre de domino creado al comienzo de la Internet ya se encuentra en su versión 9, una versión muy estable y que gracias a la libertad de su código ha avanzado vertiginosamente librándose de innumerables vulnerabilidades constituyendo actualmente una de las mejores base de datos distribuida y jerárquica que almacena información relativa a los nombres de dominio en internet o gestiona nombres de equipos y servicios en redes locales; se puede citar como ejemplo de la gran magnitud usabilidad a nivel internacional de este servidor las pruebas realizadas por el sitio http://dns.measurement-factory.com/ especializado en tareas de recaudación de estadísticas en octubre del 2007, donde fueron comprobados 386 588 dominios de internet , de los cuales el 64% usaba la versión 9 de BIND para “resolver” sus nombres de dominio, otras estadísticas sobre el uso del mismo y comparativas entre uso de servidores DNS pueden ser comprobadas en la web de netcraft.

¿CÓMO MIGRAR EL DNS HACIA BIND?

Existen diferentes vías para migrar un servidor DNS desde Windows hacia GNU/LINUX. Si existe un número pequeño de entradas del DNS, la migración se puede efectuar copiando y pegando la información, ya que está puede obtenerse en el Microsoft DNS Manager o en el archivo (.dns) que se encuentra en:

C:\WINNT\system32\dns

Sin embargo este método puede consumir mucho tiempo si se tratase de muchas entradas. Para muchos la forma más fácil de transferir la información es usando el mecanismo de "transferencia de zona", bastante útil y efectiva. Otra de las formas es haciendo uso de algunos script que interpretan la configuración en el servidor de Windows y generan la configuración para BIND, uno de ellos es:

w2lmt-migrate-dns

El cual se puede descargar a través de la web y pertenece a un conjunto de scripts realizados a raíz de la publicación del libro: "Windows to GNU/Linux migration toolkit" de David Allen, los mismos se encuentran disponibles a través de la URL que se mostrará al final de la explicación. Este método automatiza el proceso, lo hace más rápido y factible cuando se tiene un gran número de entradas. Para el uso de este script lo primero a tener en cuenta será configurar el archivo llamado *migrate-dns.conf*; con la configuración de este archivo se obtienen las bases de datos del servidor de dominio, las cuales serán almacenadas en una dirección especificada. Posteriormente se ejecuta el comando:

w2lmt-migrate-dns -f migrate-dns.conf

Con esto ya se tiene una copia de nuestro DNS. Se debe tener en cuenta, que en el servidor al cual se le quiere hacer una réplica de los registros hay que permitir a través de la herramienta administrativa usada para el mismo transferir sus zonas hacia el host especificado. Después y una vez ejecutados los scripts de migración se configura nuestro DNS previamente instalado con los datos adquiridos. Teniendo en cuenta que es muy posible que se tenga que modificar los registros SOA y NS producto del nuevo cambio de servidor (dirección ip).

MIGRACIÓN HACIA UN SERVIDOR LDAP

La propuesta de migración de un Active Directory hacia un servidor libre se basa en la implementación libre del protocolo de acceso ligero a directorios más conocida como OpenLDAP. El mismo es un servicio de directorio que, entre otras cosas, permite contener los datos (logins, claves) de una serie de usuarios y realizar la autentificación en máquinas clientes a través de un único servidor OpenLDAP. A continuación se enumeran una serie de características que son el motivo de la propuesta de dicho servidor:

1. Es muy rápido en la lectura de registros.
2. Permite replicar el servidor de forma muy sencilla y económica.
3. Muchas aplicaciones de todo tipo tienen interfaces de conexión hacia OpenLDAP y se pueden integrar fácilmente.
4. Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas.
5. Usa un sistema jerárquico de almacenamiento de información.
6. Permite múltiples directorios independientes.
7. Funciona sobre TCP/IP y SSL.
8. Es un servidor fácil de instalar, mantener y optimizar.
9. Proporciona respuestas rápidas a operaciones de búsqueda o consulta.
10. Tiene la capacidad de replicar información, con lo que aumenta la disponibilidad y fiabilidad de la información, reduciendo además el tiempo de respuesta.

11. Presenta varios clientes que permiten una interfaz gráfica amigable del mismo.
12. Combinado con Samba, puede ser usado como controlador de dominio cumpliendo muchas de las exigencias del Active Directory.

Acerca de las razones expuestas anteriormente, se puede plantear de este protocolo para mantener e intercambiar información almacenada en directorios con grandes funcionalidades y provisto de una implementación libre, que es en muchísimos aspectos, una herramienta potente que cumple su función, brindando grandes oportunidades a quienes deseen realizar la migración de cualquier organización, contando además con elevados niveles de eficiencia, seguridad y posibilidades de automatización.

¿CÓMO MIGRAR EL ACTIVE DIRECTORY?

Para lograr la migración desde un servicio de directorios activo de Windows Server 2003 hacia un OpenLDAP de GNU/Linux, se hace necesario primeramente lograr la instalación de un controlador de dominio primario con Samba, para permitir el acceso al mismo por cualquier tipo de plataforma que usen los clientes, ya sea Windows o GNU/Linux.

¿Cómo realizar la migración?

Lo primero, como se explica anteriormente, es crear el controlador de dominio, esto se hará a través de scripts implementados en Perl (pudieran estar implementados en otro lenguaje), que permitirán conectarse al controlador de dominio primario (PDC) sobre Windows y hacer una salva del mismo a través de Samba que debe estar configurada como BDC. Los pasos a seguir para lograr este objetivo son:

1. Instalar y configurar adecuadamente el servidor Openldap teniendo en cuenta que se creará el controlador de dominios a través de Samba.
2. Configurar el mecanismo de autenticación de la máquina que está siendo usada como servidor, para de esta forma usar el servicio de autentificación de los usuarios a través del protocolo LDAP.
3. Instalar y configurar Samba teniendo en cuenta que será usado como controlador de dominio secundario (BDC), o controlador de dominio que será usado para realizar una copia del Active Directory sobre Windows Server.
4. Instalar smbldaptools para proveer de esta forma las herramientas necesarias para lograr establecer la comunicación entre Samba y Openldap. No es necesario la configuración de las mismas pues este proceso se automatizará.
5. Configurar los scripts de acuerdo a las características del Active Directory, es decir, el IP del mismo, la base de búsqueda y demás.

Ya debemos estar listos para comenzar el proceso de migración de la forma más segura posible. Para ello hay que asegurar que Samba no esté ejecutándose, y si lo esté Openldap, luego se procede a ejecutarlos.

Llegado este momento, ya se debe estar listo para convertir al servidor Samba en controlador de dominio. Para ello es necesario activarlo por uno mismo en el servidor y reiniciarlo.

Una vez migrado el directorio activo, es posible que algunos servicios que autentiquen contra el antiguo Active Directory, sea necesario modificarles algunas configuraciones para que funcionen correctamente, lo cual seria conveniente evaluar antes de la migración y cambiar las configuraciones de estos servicios simultáneamente. También vale aclarar que en el momento de producirse la migración del Active Directory, estos servicios que autenticaron con el antiguo, y que aun continúan sobre Windows Server es necesario que cuanto antes sean reemplazados por soluciones libres sobre GNU/Linux, tal es el caso de las aplicaciones web, servicios de mensajería instantánea, servidores ftp, de correo y proxy.)

MIGRACIÓN HACIA UN SERVIDOR DHCP

DHCP es un protocolo que permite que las máquinas obtengan sus datos de red en tiempo de arranque a partir de un servidor central o varios El DHCP permite el uso eficaz de direcciones IP y reasignará las direcciones siempre que sea posible. También permite la administración central de muchas direcciones globales como servidores de portales y nombres.

MIGRANDO EL DHCP

La alternativa libre propuesta para este servidor es el dhcp3-server.

El primer paso para migrar DHCP desde Windows hacia GNU/Linux consiste en determinar todos los ámbitos así como las propiedades de cada uno de ellos, esto se efectúa a través de la interfaz de administración del servidor DHCP, donde hay que encontrar los ámbitos que tenemos en nuestro servidor y obtener la información de cada uno de ellos. Esta información la guardamos en un fichero o bien la podemos anotar en una hoja de papel. Después de recolectar toda la información de los ámbitos entonces se procede a configurar el DHCP en GNU/Linux. Este proceso puede automatizarse, ahorrando mucho más tiempo y consiste en ir al servidor y exportar la lista de ámbitos desde la herramienta que permite administrar el servidor de dhcp; con esta lista de ámbitos, algo muy sencillo y viable es hacer un pequeño script en perl u otro lenguaje, que con esta información coloque todos los parámetros necesarios para que el nuevo servidor de DHCP sobre GNU/Linux lo use. La parte de la configuración consiste en editar el fichero dhcpd.conf con la información de los ámbitos, información que se introduce a través del script anteriormente mencionado. Por último se reinicia el servicio y se comprueba que el DHCP que se montó sobre GNU/LINUX es funcional. Pruebas realizadas con este sistema han sido satisfactorias en grandes redes de computadoras.

MIGRACIÓN DEL SERVIDOR DE CORREO

Existen varias alternativas libres, que pudieran utilizarce con buenos resultados, la elección de uno u otro depende de las características del sistema de correo que pretenda utilizar, así como de la experiencia del administrador encargado a instalarlo.

Como agentes de transporte de correo electrónico (MTA) están: Sendmail[6], Qmail[7], Postfix[8] y Exim[9] entre otros, estos hacen uso del protocolo SMTP (Protocolo Simple de Transferencia de Correo) para el intercambio de correo. Cada uno tiene sus caracteríticas y ventajas, los más populares son los 3 primeros.

Sendmail, fue uno de los primeros en desarrollarse y constituye prácticamente un estándar, y es precisamente la razón por la cual otros ofrecen compatibilidad con este, tales como Postfix quien a su vez es uno de los mas seguros.

La propuesta de los autores se basa sobre Postfix como MTA, por las razones que se describen a continuación:

- Configuración sencilla y bastante flexible.
- Estabilidad, seguridad y capacidad ilimitada de cuentas.
- Facilidad de configuración, (no siendo así en Sendmail).
- Integración sencilla con las aplicaciones para correo electrónico (como pueden ser los clientes de correo).
- Se le pueden incluir listas de correo, antivirus, anti spam, interface webmail, entre otros elementos.
- Servidor de correo modular y cada módulo tiene una tarea diferente con un mínimo intercambio de información entre ellos, lo que aumenta su seguridad.
- Posee tablas de acceso rápido en múltiples formatos y tiene una gran integración con Ldap, Mysql, PostgreSQL y diversas bases de datos relacionales.
- Soporta TLS (Transport Layer Security), mbox, maildir, dominios virtuales, SASL y reescritura de dirección; y una gran capacidad para manejar altos volúmenes de correo.

Una buena combinación para obtener un servidor de correo es Potsfix como servidor de correo SMTP, Cyrus-SASL como servidor POP/IMAP con SSL, squirrelmail como servidor de Webmail, Clamav+Amavis-new como sistema de antivirus, y Postfix VDA para dar cuotas de disco a los buzones.

En los lugares donde aun exista el servidor correos Microsoft Exchange y por políticas de la entidad haya que mantener dicho servicio, se puede usar la alternativa de código abierto Open-Xchange, que es la solución de trabajo en grupo open source más utilizada en todo el mundo. Con la migración a este servidor se podrán mantener los datos de los usuarios y el cambio será transparente para ellos, podrán continuar usando sus clientes de correo como Outlook o Thunderbird y disfrutar de ventajas como mensajería instantánea, gestión de proyectos, interfaz personalizable, carpetas compartidas, conexión en tiempo real con el servidor para acelerar la comunicación.

MIGRACIÓN DE UN SERVIDOR PROXY

Para proponer un plan de migración hacia un servidor proxy libre se mencionarán varios de los que existen en el mundo: NTLMAPS, Privoxy y Squid. En base al estudio realizado y las necesidades de la institución se propone usar Squid.

El proxy-caché squid es una excelente solución para optimizar el uso del enlace a Internet y acelerar el tráfico web ya que almacena los contenidos más frecuentemente accedidos. Brinda además mecanismos muy flexibles para administrar el acceso por usuarios, equipos, URLs, tipo de contenido y demás. Soporta la utilización de distintos filtros de contenido, algunos de los cuales permiten la utilización de "listas negras" de acceso público que contienen listados de sitios clasificados por categoría (pornografía, juegos violentos, etc). Posee herramientas de generación de reportes que permiten visualizar de forma flexible el acceso a la web, discriminando usuarios, sitios, horarios y brindando información muy detallada.

MIGRACIÓN DE UN SERVIDOR WEB

En el mundo existen varios servidores web libres, entre los cuales están: Apache, Xitami, Thttp, PublicFile.

Sin dudas Apache es uno de los servidores web más usados de todo el mundo. Aproximadamente el 50% de los servidores de la red utilizan Apache según las estadísticas históricas y de uso diario proporcionadas por el sitio www.netcraft.com. El servidor Apache se basa en el modelo clásico de cliente-servidor. Algunas claves para su éxito son su modularidad, potencia y disponibilidad; de forma general al igual que todos los productos modulares consiste de una aplicación constituida por un núcleo básico que cumple con las características elementales de un servidor web y un conjunto de módulos para extender las funcionalidades del mismo, ejemplos de importantes módulos son: mod_perl, un interprete de Perl empotrado en Apache y jakarta un potente servidor de aplicaciones.

Entre las propiedades y características de Apache por las cuales se propone la migración hacia dicho servidor libre son: simplicidad, admite la última versión del HTTP/1.1, puede trabajar con CGI y/o con docenas de módulos nativos que existen para el mismo, muchas veces resulta útil el trabajo con módulos CGI pero otras veces por motivos de seguridad se puede usar módulos nativos, en estos cosas valdría la pena comparar elementos tan esenciales como la seguridad, la rapidez y ver que se desea lograr, el uso de uno u otro dependerá también de la disponibilidad de los mismos para la ejecución de la tarea en cuestión; admite servidores virtuales, autenticación HTTP, cuenta con un servidor proxy, sus registros son muy personalizables y también brinda gran información sobre el estado del servidor. Apache presenta entre otras características mensajes de error altamente configurables, bases de datos de autenticación y negociado de contenido. La mayoría de las vulnerabilidades de la seguridad descubiertas y resueltas tan sólo pueden ser aprovechadas por usuarios locales y no remotamente, además de que tiene soporte para SSL lo que constituye una gran ventaja desde el punto de vista de su seguridad como servidor web.

3. SEGURIDAD

Toda red privada que usa servidores para la conexión de sus usuarios a la red y para el trabajo interno de la institución a la cual se rige, debe contar con respaldos o salvas que de forma automática permitan la seguridad e

integridad de los datos e información. Cuando se habla de integridad de salvas de datos e integridad de la información, se hace referencia a los datos de los usuarios en los servidores, e incluso en sus ordenadores, garantizando que cada usuario pueda tener acceso solo a su información, es decir que se mantenga la confidencialidad a través del uso de protocolos que proporcionen seguridad a los mismos.

Para lograr el objetivo trazado en esta investigación se ha llevado a cabo un estudio acerca de las herramientas y métodos que permiten lograr escalabilidad y flexibilidad de manera segura en el proceso de respaldo y salvas de datos e información, así como el establecimiento de medidas de seguridad que brinden la confidencialidad necesaria para llevar a cabo el trabajo continuo en la institución (más detalles en las políticas de seguridad del ministerio). Los mismos se mencionan a continuación:

MÉTODOS

1- Uso de protocolos seguros y métodos para el manejo de certificados para evitar el envío de contraseñas en un texto claro sobre la red.
Se hará uso de protocolos seguros como ssh para la conexión remota a los servidores, y ssl para el manejo de certificados, el cual proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.
2- Copias de seguridad e integridad de los datos.
Se debe establecer un mecanismo de respaldo que se realice de forma automática. El mismo debe ser ejecutado en todos los servidores que guardan datos de los usuarios, como los servidores de transferencia de archivos y de bases de datos. Además se debe realizar el respaldo de la configuración de los servidores y de la información que brindan los mismos como es el caso de los servidores web. Es importante tener en cuenta que los procedimientos anteriormente mencionados deben ser ejecutados en horas en que el tráfico de la red sea lo mejor posible para evitar la pérdida de datos.
3- Respaldo de los servidores.
El respaldo de servidores se debe de asegurar con un sistema de copias de seguridad y restauración de pérdidas apropiadas, con el objetivo de evitar pérdidas inmensas de datos que puedan perjudicar el funcionamiento de los mismos. Se propone la herramienta Bacula que es de amplia usabilidad en entornos empresariales.
4- Políticas de seguridad en los ordenadores clientes.
Se deben establecer políticas de seguridad en los ordenadores de los usuarios de la institución para evitar que sean víctimas de ataques. Así como recomendar el uso de aplicaciones que envíen sus contraseñas de forma segura. Para ello se debe tener en cuenta el establecimiento de permisos restrictivos en archivos que pueden representar huecos de seguridad para el sistema, así como de una configuración acertada que permita el uso de la red y a su vez la seguridad del ordenador dentro de la misma.
5- Políticas de seguridad en los servidores.
Se deben configurar los servidores para permitir un acceso seguro a ellos y a su vez la seguridad de los mismos. Para ello es necesario tener en cuenta aspectos como: un esquema de particionado que cumpla con la funcionalidad del servidor, una configuración detallada del firewall, el establecimiento de permisos restrictivos en archivos que puedan representar huecos de seguridad para el sistema y una configuración personalizada de los mismos así como permitir que las aplicaciones del servidor se escuchen a través de puertos y protocolos seguros, y establecer una configuración avanzada de los mismos estableciendo para ello solo los permisos necesarios, de tal forma que se brinden los servicios deseados y se obtenga la mayor seguridad posible. También es necesario contar con sistemas de detección de intrusos que permitan monitorear nuestra red y sacar conclusiones acerca del tráfico de la misma, así como de la sobrecarga de los servidores.
6- Bloqueo de los ficheros de configuración.
Se utilizará el comando chattr para marcar con una bandera los ficheros de configuración del sistema como inalterables y así aumentar la seguridad y confidencialidad de los mismos.
7- Comprobación de la integridad del sistema de ficheros.
Hacer uso de aplicaciones que permitan verificar la integridad de la información almacenada en los ficheros, como Tripwire. Para detectar cualquier cambio en el sistema de ficheros, el programa ejecuta varios checksums de todos los binarios importantes y ficheros de configuración, y los compara con una base de datos con valores de

referencia aceptados como válidos. Además se recomienda que todos los scripts o binarios que ejecute el root tengan como propietario al usuario root y se almacenen en un directorio de su propiedad.
8- Comprobación de la integridad de las contraseñas.
Utilizar programas de fuerza bruta para comprobar la fortaleza de las claves.
9- Comprobación de la seguridad del sistema.
Emplear herramientas para detectar las vulnerabilidades como es el caso de Nessus o Snort.
10- Utilización del filtrado de paquetes para restringir el tráfico de entrada y salida.
Los firewalls de filtrado de paquetes leen cada paquete de datos que pasa dentro y fuera de una LAN. Puede leer y procesar paquetes de acuerdo a la información de la cabecera y filtra el paquete basado en un conjunto de reglas programables implementadas por el administrador del firewall. El kernel de GNU/Linux tiene una funcionalidad de filtrado de paquetes embebida a través del subsistema del kernel netfilter.

Además se propone utilizar herramientas con tecnologías de encriptación para administrar los equipos del dominio (los autores de la presente investigación proponen el uso de SSH), para evitar que la contraseña del root u otra información sensible sea enviada por la red en texto plano.

HERRAMIENTAS PARA LA SEGURIDAD

Snort: Es un IDS o Sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc. conocidos. Todo esto en tiempo real. Está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/GNU/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.
Nessus: Es la herramienta de evaluación de seguridad open source de mayor renombre, es un escáner de seguridad remoto para GNU/ /Linux, BSD, Solaris y Otros Unix. Está basado en plug-in (s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad.
SSH: Una manera segura de acceder a computadoras remotas. Un reemplazo seguro para los comandos "r" (rlogin/rsh/rcp). OpenSSH deriva de la versión de ssh de OpenBSD, que a su vez deriva del código de ssh pero de tiempos anteriores a que la licencia de ssh se cambiara por una no libre. Provee de comunicaciones cifradas y seguras entre dos hosts no confiables sobre una red insegura. También se pueden redirigir conexiones de X11 y puertos arbitrarios de TCP/IP sobre este canal seguro. La intención de esta herramienta es la de reemplazar a `rlogin', `rsh' y `rcp', y puede ser usada para proveer de `rdist', y `rsync' sobre una canal de comunicación seguro. También con este protocolo puede hacerse uso de SSHFS, que es un sistemas de archivo que permite compartir carpetas remotas de un servidor de ssh; SCP para realizar copias seguras, donde los datos son cifrados durante la transferencia; y SFTP que utiliza el protocolo de transferencias de archivo seguro, utilizado normalmente con SSH para asegurar la transferencia.
Netfilter: Es un poderoso filtro de paquetes el cual es implementado en el kernel GNU/Linux estándar. La herramienta Iptables es utilizada para la configuración. Actualmente soporta filtrado de paquetes stateless o statefull, y todos los diferentes tipos de NAT (Network Address Translation) y modificación de paquetes. A su uso se puede adicionar además el de varios parches del mismo distribuido por desarrolladores del Netfilter para Path-O-Matic, lo cual le daría fortaleza a la seguridad del sistema.
OpenSSL: Es un esfuerzo de cooperación para desarrollar un set de herramientas robusto, de nivel comercial, completo en características, y open source implementando los protocolos "Secure Sockets Layer" (SSL v2/v3) y "Transport Layer Security" (TLS v1) así como también una biblioteca de cifrado de propósito general potente, además posee una amplia gama de los algoritmos criptográficos usados en muchísimos servidores web a nivel mundial, por lo cual es muy aconsejable poder usarlo en la entidad en la cual se va a realizar la migración, pues entre muchas otras funcionalidades ofrece: cifrado de datos, autentificación de servidores, integridad de mensajes y autentificación opcional de usuario; basándose para ello en la criptografía de claves simétricas y asimétricas , códigos de autentificación de mensajes (MACs) y certificados digitales x.509 y muchísimos más.

Tripwire: Es una herramienta open source para la seguridad e integridad de los datos. Tripwire es útil para monitorizar y alertar de cambios específicos de ficheros en un rango de sistemas. Para mejor eficacia, se recomienda instalar el programa antes de haber conectado el computador por primera vez a Internet a fin de crear una base de datos de los ficheros existentes en el sistema, para poder contrastar los posibles cambios en éstos una vez conectados a la red.
Nagios: Es un sistema de monitorización de equipos y de servicios de red, creado para ayudar a los administradores a tener siempre el control de qué está pasando en la red que administran y conocer los problemas que ocurren en la infraestructura antes de que los usuarios de la misma los perciban. Es un sistema complejo y completo en cuanto a sus características. La información es mostrada a través de la web. Monitoriza los hosts y servicios que se especifiquen, alertando cuando el comportamiento de la red no es el deseado y nuevamente cuando vuelve a su estado correcto. Con Nagios es posible conocer en cada momento, cuáles máquinas y dispositivos están encendidos o apagados, cuáles están fallando, cuáles funcionan correctamente, qué servicios van bien y cuáles van mal; en resumen, sirve para mirar el estado casi en tiempo real de una red, sea grande o pequeña. Fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix. Está licenciada bajo la GNU General Public License Versión 2 publicada por la Free Software Foundation.

4. ACTUALIZACIÓN, ADECUACIÓN TECNOLÓGICA Y MANTENIMIENTO

La sustentabilidad económica que permita la actualización, adecuación tecnológica y mantenimiento de los sistemas informáticos en los servidores se hace muy necesaria, pues debe tenerse en cuenta que con el avance vertiginoso de la informática, los programas de los servidores cada día brindan mayores funcionalidades a los usuarios y esto hace posible que los mismos puedan tener mayor posibilidad de comodidad y seguridad frente a un ordenador.
A medida que estas aplicaciones de servidor van perfeccionándose también van apareciendo debilidades en los anteriores, que los hacen ir caducando. La actualización de los sistemas informáticos en ocasiones sale costosa, pero usando un sistema GNU/Linux no es ningún inconveniente, pues es totalmente libre y posibilita no solo la actualización del software que se necesita, sino la adaptación del mismo a los requerimientos y necesidades.
Para ello se debe usar el sistema de repositorios, el cual brindará todas las aplicaciones que usa la distribución sobre la cual se procederá a la migración de los servidores, el mismo debe brindar la posibilidad de actualizarse directamente desde los repositorios internacionales.

La réplica de la actualización de los repositorios se realizará de forma automática y en los horarios y días acordados, y permitirá como se ha dicho anteriormente la actualización de los programas del servidor, lo cual hará posible la adecuación tecnológica de los mismos de la forma más económica posible, así como su mantenimiento.

5. CONCLUSIONES

Sin duda alguna el software libre es una alternativa viable para todas las entidades, empresas y países, en el área de administración de redes y servicio de servidores ofrece una gran cantidad de programas robustos, fiables y seguros. Existe un rechazo inicial debido a lo complicado que resulta la configuración de algunos servicios de servidores, situación esta que se puede solucionar empleando *Webmin,* una herramienta de configuración vía web que permite administrar sistemas Unix usando un navegador, sin descartar la posibilidad de hacerlo a través de los ficheros de configuración de cada aplicación.

Una de las principales dificultades que los administradores de red se encuentran es realizar la migración de servicios de servidores, que tradicionalmente se han realizados a mano, reescribiendo la configuración de los mismos, con esta propuesta se automatiza esta tarea y se realiza este proceso más rápido y eficiente, las mismas fueron probadas por los autores. Esta investigación ha impulsado el desarrollo de asistentes de migración, que permitirán a usuarios no tan expertos en la materia poder cambiar toda una plataforma de servidores Windows Servers a Sistemas operativos GNU/Linux.

Las aplicaciones propuestas que ofrecerán los servicios telemáticos, trabajan con gran robustez, fiabilidad y seguridad, y bajo los principios del software libre, solución única para alcanzar la soberanía tecnológica.

REFERENCIAS

1. Allen, David. Windows to Linux Migration Toolkit. Syngress 2004. ISBN:1931836396
2. Ed Bradford, Lou. Linux and Windows Interoperability Guide. s.l. : Prentice Hall PTR, 2002. ISBN 0130324779.
3. Esteve, Josep Jorba y Boldrito, Remo Suppi. Administración Avanzada de GNU/Linux. Barcelona : UOC Formación de Postgrado, 2006. ISBN: 84-9788-116-8.
4. Nemeth, Evi, Garth, Snyder y Hein, Trent R. Linux Administration Handbook. s.l. : Addison-Wesley Professional, 2006. ISBN 0131480049.
5. Barceló Ordinas, José María, Íñigo Griera, Jordi y Ramón Martí Escalé, Ramón Martí Escalé. Redes de Computadores. Barcelona : UOC Formación de Postgrado, 2006. ISBN: 84-9788-117-6.
6. Bryan Costales, Eric Allman. Sendmail, Third Edition. O'Reilly 2002. ISBN: 1565928393
7. John R. Levine. QMAIL. O'Reilly 1999. ISBN: 1565926285
8. Ralf Hildebrandt, Patrick Koetter. State-of-the-Art Message Transport. 2005. ISBN: 1593270011
9. Philip Hazel. EXIM. O'Reilly 2001. ISBN-10: 0596000987
10. Tom Adelstein & Bill Lubanovic. Linux System Administration. O'Reilly 2007. ISBN-10: 0-596-00952-6

Fuente electrónica

1. Sitio web de Snort. [Disponible en: http://www.snort.org/]
2. Sitio web de Nessus. [Disponible en: http://www.nessus.org/]
3. Sitio web de Nagios. [Disponible en: http://www.nagios.org/]
4. Sitio web de OpenSSH. [Disponible en: http://www.openssh.com/]
5. Sitio web de OpenSSL. [Disponible en: http://www.openssl.org/]
6. Sitio web de Open-Xchange. [Disponible en http://www.open-xchange.com]

Autorización y Renuncia

Los autores autorizan a LACCEI para publicar el escrito en los procedimientos de la conferencia. LACCEI o los editores no son responsables ni por el contenido ni por las implicaciones de lo que está expresado en el escrito

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.